Fecha de Emisión del Informe: 24-11-2022

Proceso auditado:	**GESTIÓN DE TICS**
Dependencia auditada:	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Nombre y cargo del responsable del proceso / dependencia auditada:	LEYDY YOHANA PINEDA – JEFE OFICINA
Equipo auditor:	ANA YANCY URBANO VELASCO
Fechas de Ejecución de la Auditoría:	Fecha de Apertura: 28-09-2022 Fecha de Cierre: 11-11-2022

Objetivo de la auditoría	Evaluar la política de Seguridad de la Información de la SDM, según selectivo.
Alcance de la Auditoría:	Se verificará según selectivo a los procesos definidos en el alcance de la política lo cuales se detallan a continuación: *Misionales (• Planeación de Transporte e Infraestructura; Gestión de Tránsito, y Control de Tránsito y Transporte; Ingeniería de Tránsito; Gestión de Trámites y Servicios para la Ciudadanía; Gestión Contravencional y al Transporte Público, Gestión Social y de Apoyo que tiene la SDM. Y proceso de apoyo: • Gestión de TICs; •Gestión Administrativa; • Gestión del Talento Humano, • Gestión Financiera Basada en información generada entre el período comprendido entre el 01/01/2021 y el 31/08/2022
Criterios de la Auditoría:	PA04-P01 Política General del Sistema de Gestión de Seguridad de la Información SDM PE01-M01 Manual del Modelo Integrado de Planeación y Gestión de la Secretaría Distrital de Movilidad. Demás documentación que haga parte del tema.
Declaración del Auditor o Equipo Auditor.	En el desarrollo de la presente auditoría, el auditor o equipo de auditoría no fue sujeto de presiones indebidas, no presentó ningún tipo de impedimento que afecta su objetividad, actuó con el debido cuidado profesional y bajo los principios éticos y reglas de conducta del estatuto de auditoría.

Nota: Los pies de página y el ejemplo planteado, son elementos orientadores al momento de elaborar el respectivo informe, por favor en la versión final del informe no los incluya.

RESUMEN EJECUTIVO[1]

Tipo de Hallazgo	Cantidad
Hallazgo (No conformidad)	01
Observación	03
Total	04

DESARROLLO DE LA AUDITORÍA[2]

RESULTADOS

N° NC	DESCRIPCIÓN
NC 1	Verificados los mapas de riesgos de gestión de la entidad, se evidenció que no tienen a la fecha identificados riesgos de seguridad de la información para todos los procesos definidos en el alcance del sistema (sólo OTI), lo cual incumple lo estipulado en la *"Política General del Sistema de Gestión de Seguridad de la Información Secretaría Distrital de Movilidad" con código: PA04-P01 y versión:1 de fecha 09-12-2021",* respecto del principio "*Los riesgos de seguridad de la información definidos en cada uno de los procesos incluidos dentro del alcance del SGSI, deberán ser tratados y gestionados en conjunto con las dependencias de cada proceso y la Oficina de Tecnologías de la Información y las Comunicaciones*". Lo anterior, debido posiblemente a que no han impartido la directriz y despliegue de la política, para que definan y controlen en cada proceso los riesgos de seguridad de la información. Lo anterior, conlleva a materializar el riesgo *"Posibilidad de afectación reputacional por aumento de Incidentes de seguridad en la plataforma tecnológica y requerimientos de los usuarios internos debido a la gestión del Subsistema de Gestión de Seguridad de la Información fuera de los lineamientos procedimentales*" y con ello la posible vulneración de los atributos de confidencialidad, integridad y disponibilidad de la información.

OBSERVACIONES

[1] Describa en un párrafo no mayor a 6 líneas el resultado de la auditoría realizada.

[2] Relación clara y dimensionada de las conclusiones y recomendaciones derivadas de las pruebas o procedimientos de auditoría desarrollados. En este espacio, registre la metodología (Reunión de Apertura, Entrevistas, Encuestas etc.), muestra, limitaciones y en sí los aspectos revisados.

N° Observación	DESCRIPCIÓN
OB 1	Se observó que la entidad cuenta con un plan espejo para los diferentes servidores de la Entidad; sin embargo, estos se encuentran en el mismo sitio y espacio geográfico, lo cual puede conllevar a la materialización del riesgo "*Posibilidad de afectación reputaciones por aumento de requerimientos de los usuarios internos y externos solicitando la atención a sus necesidades y aumento de quejas debido a la gestiona del plan de continuidad fuera de los lineamientos técnicos",* lo anterior pudo ser generado por debilidades en la estructuración del plan de contingencia y continuidad del negocio, lo q puede conllevar a que ante una contingencia no se cuente con la capacidad de cobertura y recuperación de información y servicio ante un posible desastre que se pueda presentar en la SDM o a nivel de la ciudad de Bogotá.
OB 2	Se observó en el monitoreo de riesgos de gestión, que tienen el control de backups solicitados por los usuarios, sin embargo, no se están incluyendo en el consolidado de backups los generados de manera periódica a las bases de datos y aplicativos que utilizan en la entidad, lo cual puede conllevar al incumplimiento al anexo de la política: "Políticas específicas de seguridad y privacidad de la Información - Código: SGSI-P02, Versión: 2.0, de fecha 28 de octubre de 2020, en lo que se refiere a los roles y responsabilidades de OTI – [..] Custodiar la información y los medios de almacenamiento bajo su responsabilidad[..]". Lo anterior pudo ser ocasionado por debilidades en la aplicación del control identificado para el riesgo debido por falta de consolidación de la información y puede conllevar a la materialización de eventos de riesgo.
OB 3	Se observó que la OTIC, no tiene mapeado las zonas restringidas en las diferentes sedes y pisos de la SDM, por lo que se requiere fortalecer los controles con el fin de que no transite personal no autorizado dentro del espacio de "*Gestión de Tránsito*", donde se evidenció que aunque cuenta con cámara y biométricos allí permanecen las puertas abiertas.; lo cual puede conllevar a la materialización del riesgo de "*posible pérdida de información"*; riesgo que tampoco está identificado ni controlado según verificación del mapa de riesgos del proceso ni a nivel institucional.

En respuesta al resultado de esta auditoría del informe Preliminar, la Política de Seguridad de la Información, a través del memorando N°20221200029093 de fecha 21 de noviembre de 2022, realiza las siguientes observaciones así:

NO CONFORMIDADES:

NC 1 Verificados los mapas de riesgos de gestión de la entidad, se evidenció que no tienen a la fecha identificados riesgos de seguridad de la información para todos los procesos definidos en el alcance del sistema (sólo OTI), lo cual incumple lo estipulado en la *"Política General del Sistema de Gestión de Seguridad de la Información Secretaría Distrital de Movilidad" con código: PA04-P01 y versión:1 de fecha 09-12-2021",* respecto del principio "*Los riesgos de seguridad de la información definidos en cada uno de los procesos incluidos dentro del alcance del SGSI, deberán ser tratados y gestionados en conjunto con las dependencias de cada proceso y la Oficina de Tecnologías de la Información y las Comunicaciones*". Lo anterior, debido posiblemente a que no han impartido la directriz y despliegue de la política, para que definan y controlen en cada proceso los riesgos de seguridad de la información. Lo anterior, conlleva a materializar el riesgo *"Posibilidad de afectación reputacional por aumento de Incidentes de seguridad en la plataforma tecnológica y requerimientos de los usuarios internos debido a la gestión del Subsistema de Gestión de Seguridad de la Información fuera de los lineamientos procedimentales*" y con ello la posible vulneración de los atributos de confidencialidad, integridad y disponibilidad de la información.

Respuesta de la OTIC: Se acepta la no conformidad y se procederá a formular el respectivo plan de mejoramiento.

Respuesta del Auditor: No tiene observación alguna.

NC 2 Durante el primer semestre de 2022 la OTIC no realizó actividades de concientización ni sensibilización a todo el personal vinculado a la SDM, según lo relacionado con el sistema de Gestión de Seguridad, lo cual incumple lo estipulado en la "Políticas específicas de seguridad y privacidad de la Información - Código: SGSI-P02, Versión: 2.0, de fecha 28 de octubre de 2020.", en lo que se refiere a los descrito en los Roles y Responsabilidades para la Oficina de Tecnologías de la Información y la Comunicación, específicamente en: "Definir e implementar la estrategia de concientización y sensibilización en Seguridad de la Información para los funcionarios, contratistas y terceros". Lo anterior pudo ser generado porque no contaba con el personal suficiente para ejecutar dichas actividades, conllevando a la materialización del riesgo "Posibilidad de afectación reputacional por aumento de requerimientos de los usuarios internos solicitantes de asesoría en adquisición y cambios tecnológicos debido a la gestión del control de cambios fuera de los lineamientos procedimentales".

Respuesta de la OTIC: No se acepta la no conformidad.

La Oficina de Tecnologías de la Información y las Comunicaciones realizó en su planeación inicial, la programación de sensibilización de seguridad para el segundo semestre del 2022, donde se estimaron los cambios administrativos de personal y la continuidad al mismo, debido a la Convocatoria Distrito 4 (Concurso) de empleos de Carrera Profesional de la Comisión Nacional del Servicio Civil.

Esto soportado por el Plan Operativo Anual de Gestión de la OTIC (POA) donde se estableció la siguiente meta con actividades de Cumplimiento:
Meta 14: *Lograr que el 80 % de la evaluación sobre cultura de seguridad de la información y seguridad digital respondidas sean aprobadas.*
· Así mismo, para el presente año y de acuerdo a lo planeado para el mismo se empezaron a ejecutar las campañas de sensibilización las cuales tienen por objetivo socializar los temas de seguridad a la entidad, y esto se ha hecho a través de boletines y/o tips de seguridad enviados a través del correo electrónico institucional.
· Se envió la evaluación de seguridad por medio de formulario vía correo electrónico.
· Se realizó la campaña de phishing para todos los funcionarios con usuario de directorio activo.
· Se han realizado las jornadas de capacitación de apropiación TI y Seguridad Digital a través de conferencias realizadas por la plataforma meet.
· Se ha gestionado un curso de ciberseguridad el cual está pendiente de aprobación por parte de la Oficina de Comunicaciones de la Entidad.

Respuesta del Auditor:

Verificada la retroalimentación al hallazgo configurado en el informe preliminar, por parte de las OTIC el auditor procedió a cotejar contra la política de seguridad de la información y determinó que es procedente retirar el hallazgo del presente informe. No obstante, lo anterior se el auditor configura la siguiente recomendación:

- Realizar sensibilizaciones por parte de la OTI de manera continua para que todos los funcionarios y contratistas apropien la Política de Seguridad de la información y la aplicación de los controles para el prevenir los riesgos y asegurar los atributos de la información (integridad, disponibilidad y confiabilidad).

OBSRVACIONES:

Observación 1: Se observó que la entidad cuenta con un plan espejo para los diferentes servidores de la Entidad; sin embargo, estos se encuentran en el mismo sitio y espacio geográfico, lo cual puede conllevar a la materialización del riesgo “Posibilidad de afectación reputaciones por aumento de requerimientos de los usuarios internos y externos solicitando la atención a sus necesidades y aumento de quejas debido a la gestiona del plan de continuidad fuera de los lineamientos

técnicos", lo anterior pudo ser generado por debilidades en la estructuración del plan de contingencia y continuidad del negocio, lo que puede conllevar a que ante una contingencia no se cuente con la capacidad de cobertura y recuperación de información y servicio ante un posible desastre que se pueda presentar en la SDM o a nivel de la ciudad de Bogotá.

Respuesta de la OTIC:
Desde la Oficina se tiene estimado como proyecto para el año 2023 realizar una consultoría para la gestión de un plan de continuidad de negocio de la entidad, desde este punto y con los resultados de la misma, se podrá tener una mejor visibilidad que nos permita tener una contingencia ante un desastre que se pueda presentar.

Respuesta del Auditor:
El auditor ratifica la observación, y como lo manifiesta la OTIC se van a tomar acciones con el fin de prevenir la posible materialización del riesgo identificado.

Observación 2: Se observó en el monitoreo de riesgos de gestión, que tienen el control de backups solicitados por los usuarios, sin embargo, no se están incluyendo en el consolidado de backups los generados de manera periódica a las bases de datos y aplicativos que utilizan en la entidad, lo cual puede conllevar al incumplimiento al anexo de la política: "Políticas específicas de seguridad y privacidad de la Información - Código: SGSI-P02, Versión: 2.0, de fecha 28 de octubre de 2020, en lo que se refiere a los roles y responsabilidades de OTI – [..] Custodiar la información y los medios de almacenamiento bajo su responsabilidad[..]". Lo anterior pudo ser ocasionado por debilidades en la aplicación del control identificado para el riesgo debido por falta de consolidación de la información y puede conllevar a la materialización de eventos de riesgo.

Respuesta de la OTIC:
La Oficina de Tecnologías de la Información y las Comunicaciones cuenta con un procedimientos y formatos internos de manejo con el Operador Tecnológico de solicitud de backups y restauraciones que se realizan en la herramienta *Netbackup*.

El *backup* es solicitado por el responsable del sistema de información, aplicación, portal o servidor y allí indica el flujo de respaldo requerido (DB, Aplicación, repositorios, etc y el orden de toma de *backup* y restauración). Para evitar que se presenten eventos en los que la restauración presente fallas por incongruencia de información entre los componentes, así mismo todos los activos están sincronizados con el NTP de Microsoft.

Se realizan restauraciones periódicas de los diferentes frentes disponibles (DB, servidores windows, linux, aplicaciones, capa media, redes etc). Estas al azar para corroborar la

integridad y el éxito de las actividades, previendo eventos que puedan afectar la continuidad en la operación.

A nivel de DB funciona de la misma forma, solo que adicional se toman *backups* con RMAN ejecutados por el DBA y se alojan en repositorios de respaldo en caliente para restauraciones que requieren tiempos bajos de disponibilidad.

Respuesta del Auditor:
Si bien la entidad ya adelantó la documentación de un procedimiento para la generación de *backups*. La observación que se consigna en este informe se encuentra encaminada a que se consolide en una sola fuente de información de los diferentes *backups* que se efectúan al interior de la entidad, lo que optimizará los resultados y controles en esta materia; por lo anterior, la observación se mantiene en el presente informe.

> **Observación 3:** Se observó que la OTIC, no tiene mapeado las zonas restringidas en las diferentes sedes y pisos de la SDM, por lo que se requiere fortalecer los controles con el fin de que no transite personal no autorizado dentro del espacio de "*Gestión de Tránsito*", donde se evidenció que aunque cuenta con cámara y biométricos allí permanecen las puertas abiertas.; lo cual puede conllevar a la materialización del riesgo de "*posible pérdida de información"*; riesgo que tampoco está identificado ni controlado según verificación del mapa de riesgos del proceso ni a nivel institucional

Respuesta de la OTIC:
Se tendrá en cuenta la observación por parte de la OTIC y se realizará la gestión con la subdirección encargada para poder dar cumplimiento a la política de la observación.

Respuesta del Auditor:
El auditor ratifica la observación, como lo manifiesta la OTIC se van a tomar acciones con el fin de prevenir la posible materialización del riesgo identificado.

DETALLE DEL DESARROLLO DE LA AUDITORÍA

El presente informe se elabora conforme lo dispuesto en el *PV01-PR02- Procedimiento Auditorías de Gestión, Seguimiento y Evaluación Versión* 1.0 de 30-08-2022*,* el cual se rige bajo los lineamientos de la *Guía de auditoría interna basada en riesgos para entidades públicas.* Versión 4 del Departamento Administrativo de la Función Pública; el trabajo de Auditoría de Gestión incluyó la aplicación de:

- **Entrevistas y Cuestionarios**: Se realizó entrevistas, se desarrolló y aplicó listas de verificación de Control Interno previamente preparadas; lo anterior con el fin de

evaluar los Riesgos y Controles inmersos en el proceso de Gestión de TICS, específicamente en lo relacionado con la implementación de la normatividad vigente vinculada con el objeto del ejercicio de auditoría llevado a cabo**.**

- **Revisión de Documentos:** Se solicitó y verificó la información relacionada con el objeto de la presente auditoría, así como los documentos, informes, manuales, entre otros; publicados en la intranet de la entidad y en la página web, vinculados al objeto de la auditoría:

  https://www.movilidadbogota.gov.co/intranet/Gesti%C3%B3n%20de%20los%20Riesgos
  https://www.movilidadbogota.gov.co/intranet/PA04

- **Análisis:** Se procedió a estructurar archivos en Excel con el fin de evaluar los criterios normativos objeto de verificación y la consolidación de la información publicada por la entidad.

Por otra parte, el ejercicio de auditoría se ejecutó con la adaptación de esquemas de auditoría remota soportada en la tecnología, las conexiones, el acceso a la información, las bases de datos institucionales y entrevistas en sitio, y verificación de información, la cual fue entregada en los plazos establecidos.

Producto de la verificación a continuación, se presentan los resultados, desarrollando el objetivo de la auditoría, basada en información generada entre el período comprendido entre el 01/01/2021 y el 31/08/2022

I. REVISIÓN GENERAL DE LA POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SECRETARÍA DISTRITAL DE MOVILIDAD

La entidad cuenta en su sistema de calidad, como información documentada tales como:

1. **“**POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SECRETARÍA DISTRITAL DE MOVILIDAD” con código: PA04-P01 y Versión:1 de fecha 09-12-2021, que describe:

“[…]La política general del Sistema de Gestión de Seguridad de la Información – SGSI de la SDM, se encuentra definida e integrada en el Manual del Modelo Integrado de Planeación y Gestión – MIPG - PE01-M01, en concordancia con la misión y visión de la entidad. Esta política general debe ser de estricto cumplimiento por parte de funcionarios directos, temporales, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con la SDM desde las diferentes políticas gubernamentales, programas, planes y proyectos que deben redundar en la preservación de la seguridad y privacidad de la información de la entidad, así como

las actividades para el cumplimiento normativo del estado en el marco de la Política de Gobierno Digital que incluye el habilitador de seguridad y la política nacional de seguridad digital […]"

Por otra parte, se indica que se debe dar cumplimiento estricto a los siguientes principios:

- ***Cumplir adecuadamente los objetivos de seguridad de la información estipulados dentro del alcance del SGSI, que se presentan en el Manual del Modelo Integrado de Planeación y Gestión de la entidad. Asumir de parte de los funcionarios, contratistas y terceros el compromiso de apropiarse y realizar actividades inherentes a la protección de los activos de información que están dentro de sus responsabilidades funcionales y contractuales en la entidad; principalmente desde los principios de confidencialidad, integridad y disponibilidad de información***.

Validando este punto, el auditado indica que se ha implementado unos compromisos un documento de confidencialidad que es diligenciado y dado a conocer a los funcionarios de la entidad en el momento de ingreso a la entidad; mientras para los contratistas se contempla en uno de sus clausulados el tema confidencialidad que deben cumplir; de igual manera en los demás tipos de contratos se contempla siempre esta cláusula.

- ***Los funcionarios, contratistas y terceros que manejen, administren las diferentes plataformas digitales de la entidad deberán cumplir con las estrategias de seguridad digital implementadas para brindar confianza digital a nuestras partes interesadas.***

Se indica en referencia a este punto, que se han desarrollado sensibilizaciones sobre diferentes temas de seguridad de la información.

- ***Dar cumplimiento a los procesos, procedimientos, guías, manuales, entre otras actividades estipuladas en la entidad para operar, controlar y medir la ejecución del SGSI***.

Se indica que se aplica lo descrito en: Política General del Sistema de Gestión de Seguridad de la Información Secretaría Distrital de Movilidad; adicional de los documentos que se encuentran controlados en el sistema de gestión de calidad.

- ***Reportar por parte de los funcionarios, contratistas y terceros cualquier sospecha, anomalía o incidente de seguridad que vulnere la confidencialidad, integridad y disponibilidad a cualquiera de los activos de información de la***

entidad, ante las instancias dispuestas por los diferentes canales de comunicación de la entidad

A partir de las notas que se publican en la página Web, los funcionarios y contratistas reportan por allí los incidentes que una vez son consolidados en la base se analizan por parte de las personas designadas para tal fin, y allí se evalúa o clasifica según sea el caso.

Adicional, el auditado aporta una base de incidentes reportados en el mes de septiembre con 202 casos reportados, y se observa en el campo “comentario de la solución” se indica que una vez revisado este no se considera un ataque sin embargo se observa que se da el tratamiento al caso y se soluciona.

- ***Todas las iniciativas, planes, programas y proyectos que se generen a través de las diferentes dependencias de la entidad que contengan componente tecnológico deberán ser avaladas por la Oficina de Tecnologías de la Información y las Comunicaciones de la SDM, a fin de preservar y garantizar esquemas efectivos de seguridad de la información***.

La Oficina de Tecnologías de la Información, indica que ellos siempre hacen el acompañamiento a las dependencias en el tema tecnológico siempre y cuando los convoque a participar.

En otros casos, sólo se enteran hasta tanto se haya dado el contrato y es ahí donde se comienza a trabajar con las diferentes dependencias con el fin de poder dar trámite a estos contratos.

- ***La instancia primordial para liderar, guiar y canalizar todos los planes, programas y proyectos que involucran la seguridad de la información estarán a cargo desde profesionales de la Oficina de Tecnología de la Información y las Comunicaciones OTIC como el Oficial de Seguridad de la Información, entre otros profesionales.***

Se detecta, dentro de la auditoría que dentro de la Oficina de Tecnologías de la Información se tiene un grupo de profesionales que según su especialidad dan el acompañamiento a los diferentes temas que sean requeridos a esta oficina.

- ***Las diferentes dependencias de la entidad deberán dar cumplimiento a las Políticas específicas de seguridad y privacidad de la Información, disponibles en la intranet.***

Constantemente, la Oficina de Tecnologías de la Información genera notas sobre las políticas de seguridad y privacidad de la información como se evidenció publicaciones:

- ***Los riesgos de seguridad de la información definidos en cada uno de los procesos incluidos dentro del alcance del SGSI, deberán ser tratados y***

gestionados en conjunto con las dependencias de cada proceso y la Oficina de Tecnologías de la Información y las Comunicaciones.

A la fecha no se tienen los riesgos por proceso, se cuenta con los riesgos que han sido identificados en la Oficina de Tecnologías de la Información, y que se han determinado para cada activo que tienen a cargo.

En entrevista se comentó que se encuentran registrando a modo de piloto en el aplicativo Global Suit, los riesgos de seguridad de OTI, en este se observa que se está configurando los controles que van asociados a cada activo, y allí podrán realizar el monitoreo y seguimiento de manera más tecnificada a estos riesgos.

Este punto se puede decir que no se tiene implementado de manera general a toda la entidad, y es importante que se genere una directriz donde todos los procesos de manera juiciosa evalúen sus activos de información y puedan determinar los riesgos para cada uno de estos.

Verificados los mapas de riesgos de gestión de la entidad, se evidenció que no tienen a la fecha identificados riesgos de seguridad de la información para todos los procesos definidos en el alcance del sistema (sólo OTI), lo cual incumple lo estipulado en la *"Política General del Sistema de Gestión de Seguridad de la Información Secretaría Distrital de Movilidad" con código: PA04-P01 y versión:1 de fecha 09-12-2021",* respecto del principio "*Los riesgos de seguridad de la información definidos en cada uno de los procesos incluidos dentro del alcance del SGSI, deberán ser tratados y gestionados en conjunto con las dependencias de cada proceso y la Oficina de Tecnologías de la Información y las Comunicaciones*". Lo anterior, debido posiblemente a que no han impartido la directriz y despliegue de la política, para que definan y controlen en cada proceso los riesgos de seguridad de la información. Lo anterior, conlleva a materializar el riesgo *"Posibilidad de afectación reputacional por aumento de Incidentes de seguridad en la plataforma tecnológica y requerimientos de los usuarios internos debido a la gestión del Subsistema de Gestión de Seguridad de la Información fuera de los lineamientos procedimentales*" y con ello la posible vulneración de los atributos de confidencialidad, integridad y disponibilidad de la información

- ***Todas las dependencias de la entidad deben estar dispuestas a apoyar en las soluciones de los incidentes y/o desastres de seguridad de la información ocurridos en la entidad, para la puesta en marcha de las actividades administrativas, operativas y logísticas en el menor tiempo***

2. "Manual del Modelo Integrado de Planeación y Gestión – MIPG", con código: PE01-M01, y Versión: 11 de fecha 11 de julio de 2022, y en este se señala lo siguiente:

"[…]La entidad ha establecido la Política del SGSI en el documento PA04-P01, el cual ha sido revisado y probado por la alta dirección considerando que sea adecuada al propósito de la entidad, los requisitos legales aplicables y los determinados en la Norma ISO 27001-2013.

La política de seguridad de la información se encuentra disponible como información documentada en la intranet de la entidad, se ha comunicado a las partes interesadas según las necesidades[…]"

Con la anterior premisa se observa que en ninguno de los dos (2) documentos se encuentra claramente definida la política adoptada por la entidad.

El auditado aportó como evidencia los siguientes documentos:

- Política de seguridad y privacidad de la Información - Código: SGSI-P01- Versión: 3.0, de fecha 30 de junio de 2020, se indica que:

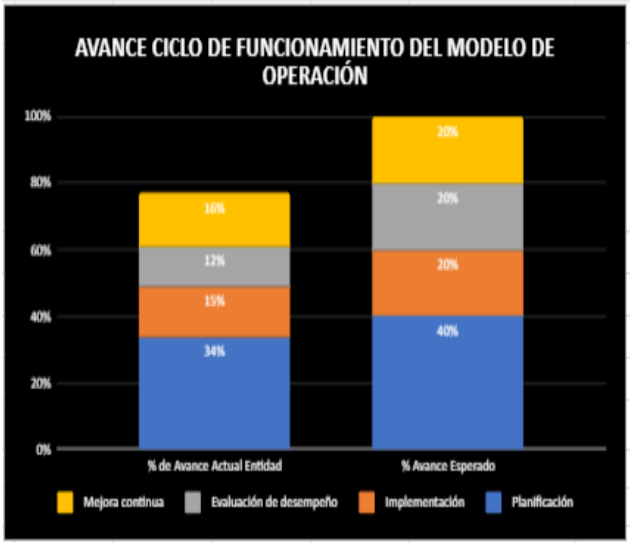
"[…]En la SECRETARÍA DISTRITAL DE MOVILIDAD (SDM), entendemos la importancia de que la información sea protegida, cualquiera que sea su forma de ser compartida, comunicada o almacenada. Buscamos promover una cultura de seguridad y buenas prácticas en el uso de las nuevas tecnologías y la gestión de los activos de información propios y de todas las partes interesadas, teniendo como premisa la información de los ciudadanos, para de esta manera, establecer un marco de confianza en el ejercicio de nuestros deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y normativas aplicables, y en concordancia con nuestra misión y visión […]"

Por lo anterior, se indaga al auditado ¿cómo se está promoviendo la cultura de seguridad y buenas prácticas?, para lo cual el auditado indica que se han planteado una serie de sensibilizaciones donde se aporta:

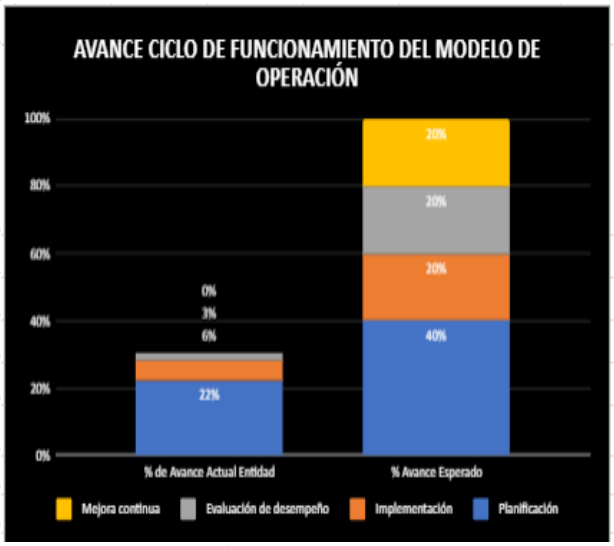
- Archivo en formato Microsoft Excel "*Plan de concientización, formación, socialización en seguridad de la información y apropiación del SGS*I". De esta evidencia se observó que se tiene programación en el mes de septiembre, octubre y noviembre.
- Archivo en formato Microsoft Excel *"Estrategia de Apropiación - Plan de concientización, socialización en TI y seguridad de la Información II Semestre de 2022*". De este archivo se observa la programación para los meses de Septiembre, Octubre, Noviembre, Diciembre, Enero, Febrero y Marzo.

Durante el primer semestre de 2022 la OTIC no realizó actividades de concientización ni sensibilización a todo el personal vinculado a la SDM, según lo relacionado con el sistema de Gestión de Seguridad, lo cual incumple lo estipulado en la "Políticas específicas de seguridad y privacidad de la Información - Código: SGSI-P02, Versión: 2.0, de fecha 28 de octubre de 2020.", en lo que se refiere a los descrito en los Roles y Responsabilidades para la Oficina de Tecnologías de la Información y la Comunicación, específicamente en: "Definir e implementar la estrategia de concientización y sensibilización en Seguridad de la Información para los funcionarios, contratistas y terceros". Lo anterior pudo ser generado porque no contaba con el personal suficiente para ejecutar dichas actividades, conllevando a la materialización del riesgo "Posibilidad de afectación reputacional por aumento de requerimientos de los usuarios internos solicitantes de asesoría en adquisición y cambios tecnológicos debido a la gestión del control de cambios fuera de los lineamientos procedimentales".

Por otra parte, se aportó como parte del avance de la implementación de la política de seguridad los resultados obtenidos en el autodiagnóstico del MSPI así:



Fuente: Resultado aplicación MSPI del 1er Semestre 2022



Resultado aplicación MSPI 2do Semestre 2021

Los anteriores resultados, permiten observar que se ha venido fortaleciendo actividades lo cual permite visualizar la mejora entre el 2do semestre de 2021 y el primer 1er semestre de la vigencia 2022.

De igual manera, se aporta por parte del auditado un documento "*Declaración de Aplicabilidad para la Seguridad de la Información SDM*", este documento no se encuentra oficialmente codificado dentro del sistema de calidad, en este se observa que la entidad va

aplicar los 114 controles que se encuentran descritos en la norma NTC ISO 27001:2013 en su Anexo A; por otra parte, se aportó el archivo "*Declaración de Aplicabilidad SMD v01.xlsx*" en este se listan todos los controles descritos en la anterior norma, y se señala por control si aplica a: Legales, Metodología de Valoración y Tratamiento de Riesgos y Entidad.

El auditado también, presenta dos (2) documentos en formato word con la propuesta de la nueva actualización de la política de Seguridad, documentos que ya fueron presentados a la Oficina Asesora de Planeación Institucional con el fin de ser aprobado una de las dos (2) versiones presentadas y de esta manera establecer una política clara a la Seguridad de la Información de la SDM.

Adicionalmente, en revisión del Sistema de Calidad se observó los siguientes documentos:

- **Políticas específicas de seguridad y privacidad de la Información - Código: SGSI-P02, Versión: 2.0, de fecha 28 de octubre de 2020**.

> […]Este documento describe las Políticas específicas de Seguridad de la Información de la Secretaría Distrital de Movilidad. Para su elaboración, se toman como base los controles y requisitos identificados en el estándar ISO/IEC 27001:2013. Las políticas incluidas en este documento se constituyen como parte fundamental del Subsistema de Gestión de Seguridad de la Información (SGSI) de la Secretaría Distrital de Movilidad y se convierten en la base para la implantación de controles, procedimientos y estándares. La Seguridad de la Información es una prioridad para la Secretaría Distrital de Movilidad y por tanto es responsabilidad de todos los funcionarios velar por el continuo cumplimiento de las políticas definidas en el presente documento. […]

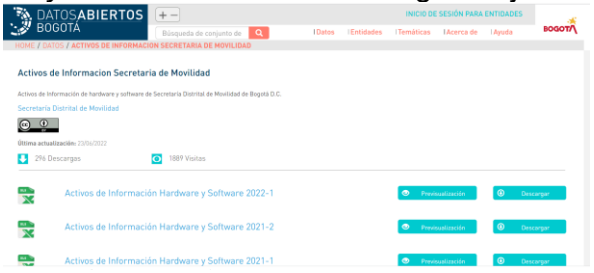
Dentro de los Roles y responsabilidades que se establecieron en este documento, se estableció para la OTI los siguientes:

ROLES Y RESPONSABILIDADES:	VALIDACIONES / OBSERVACIONES POR PARTE DEL AUDITOR
Implementar, apoyar y soportar el Sistema de Gestión de Seguridad de la Información.	El liderazgo se observa que lo lleva el Oficial de Seguridad de la Entidad.
Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de Seguridad de la Información.	Al interior, de la OTIC se realizan sensibilizaciones sobre las políticas de Seguridad, de igual manera al interior de la entidad se han realizado sensibilizaciones sobre el tema.

Administrar las herramientas tecnológicas para el cumplimiento de las políticas de Seguridad de la Información	Se cuentan con herramientas para el manejo de usuarios el Directorio Activo más demás acciones que se aplican para dar cumplimiento a las políticas específicas.
Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.	En el tema de equipos de cómputo, se observa que ningún equipo tiene garantía vigente, lo cual quiere decir que la entidad tiene una obsolescencia de equipos de un 15,46% de equipos de obsolescencia (199 equipos con fechas anteriores al 2018)
Definir e implementar la estrategia de concientización y sensibilización en Seguridad de la Información para los funcionarios, contratistas y terceros	Se evidencia que a partir del mes de septiembre se hicieron actividades de sensibilizaciones para toda la Entidad. Sin embargo, se observa que se debe realizar actividades a lo largo de toda vigencia, por lo que se debe fortalecer estas actividades.
Custodiar la información y los medios de almacenamiento bajo su Responsabilidad.	Esta actividad se realiza por un servicio SAS, para lo cual se tienen programados backup diarios, semanales y mensuales, los cuales son trasladados por el Operador todos los viernes. Esto apalanca un control que se tiene en el mapa de riesgos de este proceso y que dice "*El profesional de la OTIC y el Operador Tecnológico realiza el seguimiento constante a la ejecución de los envíos de las cintas de Backup, respaldos, y custodias por el proveedor establecido de la entidad.*" Esta actividad, fue validada con el Operador Tecnológico, el cual evidenció en visita las planillas generadas de entrega al Operador de custodia de la información. Sin embargo, en archivo aportado del mes de agosto, se observó en el monitoreo de riesgos de gestión, que tienen el control de backups solicitados por los usuarios, sin embargo, no se

	están incluyendo en el consolidado de backups los generados de manera periódica a las bases de datos y aplicativos que utilizan en la entidad, lo cual puede conllevar al incumplimiento al anexo de la política: "Políticas específicas de seguridad y privacidad de la Información - Código: SGSI-P02, Versión: 2.0, de fecha 28 de octubre de 2020, en lo que se refiere a los roles y responsabilidades de OTI – [..] Custodiar la información y los medios de almacenamiento bajo su responsabilidad[..]". Lo anterior pudo ser ocasionado por debilidades en la aplicación del control identificado para el riesgo debido por falta de consolidación de la información y puede conllevar a la materialización de eventos de riesgo. Por otra parte, si bien se tiene un procedimiento para la realización de backup, este no se encuentra debidamente formalizado en el sistema de gestión de calidad.
Definir, mantener y controlar la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las Estaciones de trabajo de los usuarios; así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software base y de aplicaciones	Para este tema el auditado comenta que se cuenta con una herramienta llamada Metrix, la cual es administrada por el Operador Tecnológico, adicional que se comenta que es un tema compartido con la Subdirección Administrativa quien es la que maneja el inventario de la Entidad en lo relacionado de lo que entra y sale del Almacén. En sitio, se observa que allí se maneja y se revisa la instalación de software permitido para la entidad y el cual apoya el licenciamiento respectivo de software en la entidad. Se solicitó un listado de software que tiene en la actualidad la entidad, y este no fue entregado por el auditado, con el fin de hacer cruce de información con la que

	es manejada por la Subdirección Administrativa.
Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.	Se tenía establecido el Contrato N° 2021-1866 con SELCOM, quien era el operador que se encarga de realizar el monitoreo y evalúa toda la plataforma tecnológica de la Entidad, para lo cual se tienen establecidas de igual manera reuniones semanales sobre el seguimiento que se efectúa, por otra parte, mensualmente se presente el Informe de gestión mensual, como evidencia se observó el informe correspondiente al mes de julio, al igual se observó el informe de supervisión respectivo que realizado por el supervisor delegado por la OTI.
Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.	Se cuenta con un plan de contingencias, bajo el despliegue de la IPv6 en la infraestructura. Se observó que la entidad cuenta con un plan espejo para los diferentes servidores de la Entidad; sin embargo, estos se encuentran en el mismo sitio y espacio geográfico, lo cual puede conllevar a la materialización del riesgo "*Posibilidad de afectación reputaciones por aumento de requerimientos de los usuarios internos y externos solicitando la atención a sus necesidades y aumento de quejas debido a la gestiona del plan de continuidad fuera de los lineamientos técnicos",* lo anterior pudo ser generado por debilidades en la estructuración del plan de contingencia y continuidad del negocio, lo q puede conllevar a que ante una contingencia no se cuente con la capacidad de cobertura y recuperación de información y servicio ante un posible desastre que se pueda

	presentar en la SDM o a nivel de la ciudad de Bogotá
Establecer, documentar y dar mantenimiento a los procedimientos de Seguridad de la Información que apliquen para la plataforma de tecnologías de información administrada por esta oficina.	En conversación con el auditado, se mencionó que se encuentran en el proceso de actualización de los documentos, políticas a nivel de seguridad de la información que se tiene junto con otros documentos que impactan en esta materia y para lo cual se apoyan también en el contrato con el Operador, quienes les ayudan a documentar algunos procedimientos de uso de la OTIC.
Gestionar los incidentes de Seguridad de la Información que se presenten en la Entidad.	Se tiene la funcionalidad en la herramienta Aranda, que los usuarios reporten incidentes, para lo cual se generan listados de estos y frente a estos casos se efectúan reuniones semanales los cuales son tratados y evaluados junto con el Operador y el Oficial de Seguridad. Dentro de lo comentado por el auditado los incidentes no han afectado la infraestructura tecnológica de la entidad.
Mantener actualizados los activos de información conforme a las dinámicas de la Entidad y realizar la publicación respectiva conforme lo señala la Ley de Transparencia y Acceso a la Información Pública.	Los activos de información son actualizados y monitoreados por el Operador, y en la página web se encuentran actualizados debidamente hasta el 1 semestre de 2022, con un contenido de 1964 activos y cuya fecha actualización corresponde al 19/05/2022, tal y como se observa en imagen adjunta.  Fuente: página web secretaria

Por otra parte, en este documento en el numeral 4. Acciones que afectan la Seguridad y Privacidad de la Información se validó que controles se aplican para:

ACCIONES QUE AFECTAN LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VALIDACIONES / OBSERVACIONES POR PARTE DEL AUDITOR
i. Dejar los computadores encendidos en horas no laborables.	No se cuenta con algún control que se indique cuales, son los equipos de uso de los funcionarios que dejan encendidos y el motivo por el cual se dejan en este estado; adicional, no se han realizado sensibilizaciones frente esta acción que puede afectar la seguridad y privacidad de la información.
ii. Permitir que personas ajenas a la Secretaría Distrital de Movilidad ingresen sin previa autorización a las áreas restringidas o donde se procese información confidencial.	La Secretaria no cuenta con el mapeo físico de las áreas restringidas, con las que cuenta en la actualidad la entidad. Por otra parte, en visita en sitio en sede Calle 13 se revisó: • **Datacenter 1er Piso**: sitio adecuado, monitoreado por cámaras de seguridad y con acceso biométrico, todos sus elementos se encuentran debidamente identificados y el administrador conoce con detalle la ubicación de sus dispositivos e importancia de cada uno de los elementos allí contenidos. • **Centro de Cableado 2do Piso** (hay dos (2) puntos). **Punto 1** (por cámaras de seguridad y con acceso biométrico, todos sus elementos se encuentran debidamente identificados y el administrador conoce con detalle la ubicación de sus dispositivos e importancia de cada uno de los elementos allí contenidos). **Punto 2** (se recomienda implementar una cámara al interior, que permita visualizar el ingreso y manipulación

	de elementos, este cuarto se encuentra también, dispuesto de más elementos que no permiten la movilización dentro de este de manera adecuada. Se tiene dispuesto también, como un almacén de elementos del Operador, se recomienda separar la disposición de estos elementos por peligros que se podrían generar en este sitio. • Gestión de Tránsito -2 piso: Se observó que la OTIC, no tiene mapeado las zonas restringidas en las diferentes sedes y pisos de la SDM, por lo que se requiere fortalecer los controles con el fin de que no transite personal no autorizado dentro del espacio de "*Gestión de Tránsito*", donde se evidenció que aunque cuenta con cámara y biométricos allí permanecen las puertas abiertas.; lo cual puede conllevar a la materialización del riesgo de "*posible pérdida de información"*; riesgo que tampoco está identificado ni controlado según verificación del mapa de riesgos del proceso ni a nivel institucional. De igual manera, se realizó inspección visual al área de Plantas eléctricas que cuenta la entidad en CL 13, estas se encuentran debidamente señalizadas y se observa el mantenimiento preventivo que se les ha realizado. Por otra parte, se mencionó que en Calle 19 hay cuatro (4) centros de cableado, los cuales no fueron visitados por el auditor.

iii. No clasificar y/o etiquetar la información.	La revisión se realizó de manera visual al visitar los sitios, lo cual no se pudo constatar en una revisión más detallada del tema.
iv. No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral.	
v. No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.	La entidad tiene un control de seguridad de la parte de impresión; el cual el usuario al dirigirse a una impresora debe digitar tu clave para la impresión para que esta se genere; en los casos que el usuario, no se acerque a una impresora al apagar el equipo se borra las impresiones enviadas. En revisión visual no se observó documentos en las impresoras de la sede Calle 13
vi. Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.	En revisión visual, en sede Calle 13, no se observó incumplimiento con este numeral.
vii. Hacer uso de la red de datos de la Secretaría Distrital de Movilidad para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.	Este control se hace a través de la herramienta de control de correo, y la herramienta firewall se hace filtrado de contenido web, políticas de destino. A través de políticas no puede acceder. Adicional, se controla el tamaño de información a enviar, y se controla en caso de registro de spam.
viii. Instalar software en la plataforma tecnológica de la Secretaría Distrital de Movilidad cuyo uso no esté autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones, y que pueda atentar contra las leyes de derechos de autor o propiedad intelectual.	No les permite autorizar la descarga de software y, por ende, no pueden instalar por que se tienen políticas de dominio. Un usuario no tiene autorización de instalación, las instalaciones se deben realizar con perfil de administrador. Sin embargo, se hace revisión a los eventos y estos son monitoreados por el gestor de seguridad. El trámite debe ser solicitado a través de ticket, y el operador le envía vía correo electrónico a OTIC la solicitud, quienes

	validan la herramienta, revisan que este licenciado y se requiere siempre y cuando este asegurado como resultado de esta revisión determinan si el software está autorizado o no, para autorizar al operador que proceda en caso de ser autorizado.
ix. Enviar información clasificada de la Entidad por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.	Está sujeto al perfil del usuario, el cual es solicitado por el jefe de área y debe ser monitoreado por el mismo.
x. Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca a la Secretaría Distrital de Movilidad.	En este punto, se encuentra la debilidad, dado que aún no se ha implementado el bloqueo de puertos, para lo cual ya se encuentran trabajando para la implementación de esta medida y aunque no se ha determinado pérdida o fuga de información, se pretende minimizar el riesgo.
xi. Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos de la Entidad sin la debida autorización.	Como política se tiene en la sede varias redes y estas se encuentran restringidas con las políticas de seguridad. En las sedes se conectan los equipos de los contratistas a los cuales previamente se les ha otorgado el permiso de trabajar en la red de la entidad.
xii. Ingresar a la red de datos de Entidad por cualquier servicio de acceso remoto sin la autorización de la Oficina de Tecnologías de la Información y las Comunicaciones.	Solo se tiene autorizado el ingreso por VPN a los funcionarios y contratistas que han autorizado los jefes de área.
xiii. Usar servicios de internet en los equipos de la Entidad, diferente al provisto por la Oficina de Tecnologías de la Información y las Comunicaciones.	Por políticas, los equipos fijos se conectan sólo por cable a red de la entidad, y es la red que se encuentra autorizada para navegar en la información de la entidad.
xiv. Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos de la Secretaría Distrital de Movilidad para beneficio personal.	Si bien los equipos se encuentran en la entidad, allí se aplican políticas empresariales; sin embargo, es el jefe de área quien debe monitorear las actividades de sus colaboradores.

xv. Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario o contratista.	Esto corresponde a la responsabilidad de cada usuario, de dar uso al usuario autorizado.
xvi. Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.	Es de responsabilidad de cada usuario, de dar uso al de los elementos entregados.
xvii. Retirar de las instalaciones de la secretaría Distrital de Movilidad computadores de escritorio, portátiles e información física o digital clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.	Es de responsabilidad de cada usuario, de dar uso al de los elementos entregados; sin embargo, se cuenta con el control de registro de equipos retirados que lleva las personas de seguridad.
xviii. Entregar, enseñar o divulgar información clasificada de la Secretaría Distrital de Movilidad a personas o entidades no autorizadas.	Es de responsabilidad de cada usuario, dar uso de la información que maneja; sin embargo, cada empleado y contratista firma el formato de confidencialidad con el fin se comprometen a no divulgar información.
xix. Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica de la Entidad o de terceras partes.	De acuerdo con conversación con el auditado no se ha detectado estas situaciones en la entidad.
xx. Ejecutar cualquier acción que difame, afecte la reputación o imagen de la Secretaría Distrital de Movilidad, o alguno de sus funcionarios, utilizando para ello la plataforma tecnológica.	De acuerdo con conversación con el auditado no se ha detectado estas situaciones en la entidad.
xxi. Realizar cambios no autorizados en la Plataforma Tecnológica de la Entidad.	De acuerdo con conversación con el auditado no se ha detectado estas situaciones en la entidad; los cambios se realizan de manera programada y OTI y el Operador son los que controlan que se estas acciones se realicen de manera coordinada.
xxii. Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.	Se tiene identificado los activos de información y estos se encuentran con un responsable quien debe velar por su debido uso y aplicación.

xxiii. Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente política de Seguridad de la Información.	De acuerdo con conversación con el auditado no se ha detectado estas situaciones en la entidad.
xxiv. Consumir alimentos y bebidas, cerca de la plataforma tecnológica.	Esta situación, se observa que no se cumple de manera estricta, es por ello que se recomienda implementar sensibilizaciones al respecto.
xxv. Conectar a la corriente regulada dispositivos diferentes a equipos de cómputo	Se tiene identifico por color naranja las tomas reguladas; sin embargo, se debe sensibilizar más a los usuarios sobre este tema.
xxvi. Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.	No se tiene el conocimiento sobre acciones tomadas en este punto.
La realización de alguna de estas prácticas u otras que afecten la Seguridad de la Información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo a los procedimientos establecidos para cada caso.	No se tienen reportes aún de acciones disciplinarias sobre el tema.

Se observa que la Secretaria Distrital de Movilidad, tiene contratado el tema de servicios, y en Informe consultado del mes de Julio para este Proveedor “Selcom”, se puede observar que en este se tiene un acuerdo de servicios para la atención de los requerimientos que surgen por la necesidad en esta materia al interior de la entidad, los tiempos se encuentran estructurados por:

- Mesa de Servicios
- Soporte técnico
- Infraestructura

En este informe se observa que se establecieron unos indicadores que se observa que su comportamiento ha sido favorable para la entidad tal y como se evidencio en el informe del mes de julio así:

INDICADOR	RESULTADO
Disponibilidad de la red LAN	99.78%
Disponibilidad del sistema telefónico	100,00%
Disponibilidad de equipos de respaldo eléctrico (UPS)	99,99%
Disponibilidad de equipos de respaldo eléctrico (Planta Eléctrica)	100,00%
Disponibilidad de sistemas de aire acondicionado	100,00%
Disponibilidad de los equipos de seguridad informática	99,80%
Disponibilidad de los servicios de servidor de dominio	100,00%
Disponibilidad de los servicios de servidor página Web	100,00%
Disponibilidad de los servicios de servidor página Intranet	100,00%
Disponibilidad de almacenamiento de información en la SAN/NAS	100,00%
Disponibilidad de Servicios tecnológicos (Total)	**99,99%**

Fuente: Informe de Gestión Mensual del Contrato 2021-1866 - Mes de Julio

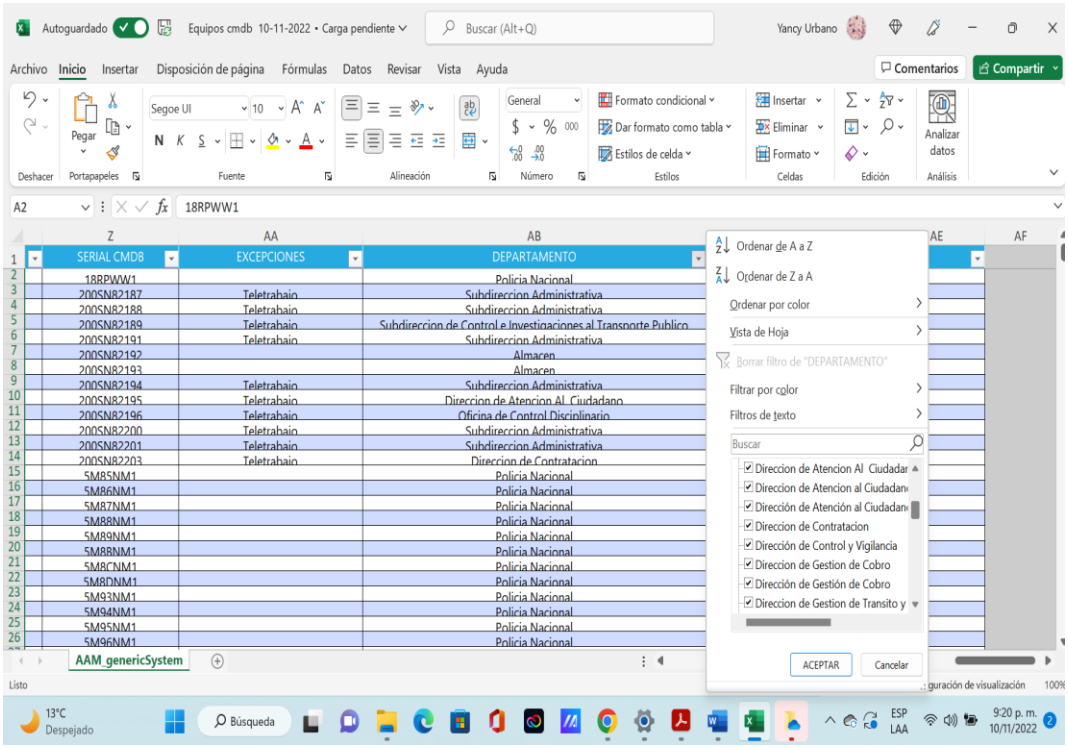
En lo que se refiera a Licenciamiento, se observa en la herramienta Matrix que esta se consolida y administra aquí tal y como se evidencia en el siguiente cuadro.

No. Contrato	Contrato	Aplicación	Licencia	Mes de vencimiento
20212189	ANTIVIRUS SOPHOS	ENDPOINT PROTECTION STANDARD, SOPHOS.	81573-SGSI RENOVACIÓN DERECHO DE USO SUBSISTEMA DE GESTIÓN	2022/Agosto
			CONSULTORÍA PARA CONFIGURACIÓN 40 HORAS	2022/Agosto
4600493181	VMWARE	VMWARE	BASIC SUPPORT/SUBSCRIPTION FOR VMWARE VREALIZEOPERATIONS 8 S	2022/Septiembre
			BASIC SUPPORT/SUBSCRIPTION FOR VMWARE VREALIZEOPERATIONS 8 S	2022/Septiembre
			BASIC SUPPORT/SUBSCRIPTION FOR VMWARE VREALIZEOPERATIONS 8 S	2022/Septiembre
			BASIC SUPPORT/SUBSCRIPTION VMWARE VCENTER SERVER 7STANDARD F	2022/Septiembre
			BASIC SUPPORT/SUBSCRIPTION FOR VMWARE VSPHERE 7ENTERPRISE PL	2022/Septiembre
			BASIC SUPPORT/SUBSCRIPTION FOR VMWARE VSPHERE 7ENTERPRISE PL	2022/Septiembre
			BASIC SUPPORT/SUBSCRIPTION FOR VMWARE VSPHERE 7ENTERPRISE PL	2022/Septiembre
20212295	ARCGIS	ARCGIS	LICENCIA - ARCGIS (ELA) CORPORATIVA	2022/Agosto
20191652	PALO ALTO	PALO ALTO	LICENCIA - PALO ALTO	2022/Agosto
20212235	OVM ORACLE	OVM ORACLE	OVM ORACLE VIRTUAL MACHINE PREMIER LIMITED 21628221	2022/Agosto
			OVM ORACLE VIRTUAL MACHINE PREMIER LIMITED (SERVERS) CSI NO.	2022/Agosto
			ORACLE LINUX PREMIER LIMITED CSI NO. 21628221	2022/Agosto
			ORACLE LINUX PREMIER LIMITED CSI NO.21628221	2022/Agosto

20212402	NAGIOS	NAGIOS	NAGIOS XI ENTERPRISE. 400-NODE LICENSE	2022/Septiembre
			NAGIOS NETWORK ANALYZER, 1	2022/Septiembre
			HORAS DE SERVICIO PARA CONFIGURACIÓN	2022/Septiembre
20212227	VISSIM Y VISUM	VISSIM Y VISUM	PTV VISSIM TAMAÑO ILIMITADO:900207410	2022/Agosto
			PTV VISSIM TAMAÑO: ILIMITADO 900207411	2022/Agosto
			PTV VISSIM TAMAÑO: ILIMITADO 900207412	2022/Agosto
			PTV VISSIM TAMAÑO: ILIMITADO 900207413	2022/Agosto
			PTV VISSIM TAMAÑO: ILIMITADO 900207414	2022/Agosto
			PTV VISSIM TAMAÑO: ILIMITADO 900207415	2022/Agosto
			PTV VISSIM TAMAÑO:ILIMITADO 900207417	2022/Agosto
			PTV VISSIM TAMAÑO: ILIMITADO 900207418	2022/Agosto
			PTV VISSIM TAMAÑO: ILIMITADO 900207419	2022/Agosto
			PTV VISSIM TAMAÑO:ILIMITADO 900207421 [2]	2022/Agosto
			PTV VISSIM TAMAÑO: ILIMITADO 900207421 [2]	2022/Agosto
		VISUM	PTV VISUM TAMAÑO: EXPERTO- GRANDE LICENCIA: 900207416	2022/Agosto
			PTV VISUM TAMAÑO: EXPERTO- GRANDE LICENCIA: 900207416	2022/Agosto
			PTV VISUM TAMAÑO: EXPERTO- PREMIUM LICENCIA: 900207420	2022/Agosto
20212188	GLOBALSUITE Y SOPHOS	GLOBALSUITE Y SOPHOS	RENOVACIÓN CENTRAL INTERCEPT X ADVANCED	2022/Agosto
			RENOVACIÓN "CENTRAL INTERCEPT X ADVANCED FOR SERVER", PARA S	2022/Agosto
			RENOVACIÓN "CENTRAL INTERCEPT X ADVANCED FOR SERVER", PARA S	2022/Agosto

Fuente: Informe de Gestión Mensual del Contrato 2021-1866 - Mes de Julio

Por otra parte, se aporta el reporte de equipos con los que cuenta la SDM; el cual contiene 1287 registros los cuales se encuentra clasificados entres Desktop y Portatiles, sin embargo, la misma información fue solicitada a la Subdirección Administrativa la cual no fue suministrada por lo cual no se realizaron pruebas de verificación entre lo registrado en esta herramienta y la contenida en el almacén de la entidad. Es importante, indicar que esta información se debe fortalecer en temas de ingreso de información tal y como se puede evidenciar en la imagen adjunta donde se evidencia el nombre de la Dependencia tiene varias alternativas de escritura, tal y como se evidencia en el pantallazo adjunto:



Fuente: archivo en formato Microsoft Excel “Equipos cmdb 10-11-2022.xlsx”

No todos los registros tienen un usuario responsable tal y como se evidencia en el siguiente pantallazo:

Proveedor	Placa	FECHA EXPIRACIÓN GARANTI	USUARIOS RESPONSABLE	NOMBRE USUARIO	USUARIO RE
	101158	12/10/2021 12:00:00 AM	Angelica Paola Zambrano Sanchez		
	101159	12/10/2021	Leyla Yazmin Cárdenas		
	101160	12/10/2021	Yenny Nataly Cruz Duarte		
	101162	12/10/2021 0:00:00	Gloria Andrea Calderon Calderon		
	101163	12/10/2021 12:00:00 AM			
	101164	12/10/2021 0:00:00	Daniel Santiago Toro Vega		
	101165	12/10/2021	Gustavo Casallas Muñoz		
	101166	12/10/2021 0:00:00	Luz Dary Rodriguez Cepeda		
	101167	12/10/2021	Misael Morales Ortiz		
	101171	12/10/2021 0:00:00	Magnolia Bejarano Espejo		
	101172	12/10/2021	Leidy Constanza Barrera Vanegas		
	101174	12/10/2021	Maria Fernanda Botia Botia		

Fuente: archivo en formato Microsoft Excel “Equipos cmdb 10-11-2022.xlsx”

IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS[3]

1. **Riesgos de Gestión**

- **Posibilidad de afectación reputacional por disminución en la evaluación por debajo del 97% de cumplimiento de los NS y aumento de quejas de usuarios debido a la realización de atención de necesidades de servicios tecnológicos fuera de los tiempos requeridos.**

Para este riesgo, se realiza seguimiento al cumplimiento a la respuesta y a la solución dada a las solicitudes y requerimientos que se atendieron en materia tecnológica con los registros en la Herramienta Aranda donde realizan seguimiento al cumplimiento y aplicación de los Niveles de servicio (NS).

- **Posibilidad de afectación reputacional por aumento de requerimientos de los usuarios internos solicitantes de asesoría en adquisición y cambios tecnológicos debido a la gestión del control de cambios fuera de los lineamientos procedimentales.**

La OTIC realiza las reuniones denominadas Comité de Cambios, donde se revisan y aprueban aquellos que no puedan afectar la infraestructura tecnológica de la entidad, esto con el fin de garantizar que las nuevas adquisiciones se ajusten a la infraestructura actual.

- **Posibilidad de afectación reputacional por aumento de requerimientos de los usuarios internos solicitando sustitución en elementos de la infraestructura TI y aumento de quejas de usuarios debido a la gestión de conceptos técnicos fuera de los lineamientos técnicos**.

La OTIC recibe solicitudes de Conceptos técnicos, en los cuales asesora a la entidad en temas relacionados con Tecnologías de la Información, con el fin de garantizar la continuidad de los servicios y aplicaciones de la entidad.

- **Posibilidad de afectación reputacional por aumento de requerimientos de los usuarios internos solicitando verificaciones en su infraestructura TI y aumento de quejas debido a la gestión de Mantenimientos Preventivos fuera de los tiempos establecidos.**

[3] Revisión y análisis cuantitativo y cualitativo del Mapa Institucional de Riesgos (MIR), así mismo, aquella situación o evento que no estando en el MIR podría materializarse de no tomar medidas oportunas ante la situación observada.

La OTIC realiza el seguimiento a la ejecución de los mantenimientos preventivos a la infraestructura tecnológica de la entidad por medio de la programación del cronograma establecidos que ejecuta el operador.

- **Posibilidad de afectación reputaciones por aumento de requerimientos de los usuarios internos y externos solicitando la atención a sus necesidades y aumento de quejas debido a la gestiona del plan de continuidad fuera de los lineamientos técnicos.**

Se realiza seguimiento a la gestión y al uso de los servicios brindados por la herramienta Suite de Google y el manejo de información en el Drive por funcionarios y contratista de la entidad que desde su sitio de trabajo o en casa hacen uso de estas funcionalidades.

- **Posibilidad de afectación reputacional por aumento de Incidentes de seguridad en la plataforma tecnológica y requerimientos de los usuarios internos debido a la gestión del Subsistema de Gestión de Seguridad de la Información fuera de los lineamientos procedimentales**.

La OTIC realiza el seguimiento a las bases de datos personales de la Entidad con memorando Orfeo solicitando a las dependencias de la entidad el reporte de las nuevas bases de datos personales que se hallan creado en esta vigencia, para que sean reportadas a la Superintendencia de Industria y Comercio (SIC), y con esta medida dar cumplimiento al uso de los datos personales.

2. Riesgos de Corrupción

- **Posibilidad de obtener una dádiva o beneficio económico para adulterar o usar de manera inadecuada los sistemas de información y la información allí depositada de la entidad con el fin favorecer a un tercero:**

La Oficina de Tecnologías de la Información y las Comunicaciones realizó seguimiento y verificación a las solicitudes en relación con la cancelación y creación de cuentas de usuario, que se solicitaron durante este periodo por los jefes de las dependencias de la SDM y supervisores designados.

- **Posibilidad de obtener una dádiva o beneficio económico por emitir un concepto técnico de para adquisición de infraestructura tecnológica (hardware y software) para favorecer a un tercero.**

La Oficina de Tecnologías de la Información y las Comunicaciones como parte de las actividades realizadas para aportar en el seguimiento a este riesgo, realiza la asignación de solicitudes de Conceptos Técnicos, solicitados por las de dependencias de la Entidad a las cuales se les da el trámite y respuesta a dichas solicitudes.

3. Riesgos de Seguridad:

AGRUPACIÓN DEL RIESGO	NIVEL DEL RIESGO			TOTAL
	Alto	Extremo	Moderado	
Cumplimiento	2	3	2	7
Cumplimiento, Imagen		3		3
Cumplimiento, Tecnológico		2		2
Cumplimiento, Tecnológico, Imagen		1		1
Estratégico		12		12
Estratégico, Operativo, Tecnológico		1		1
Estratégico, Cumplimiento	1	4		5
Estratégico, Cumplimiento, Imagen		1		1
Estratégico, Cumplimiento, Tecnológico		2		2
Estratégico, Operativo, Cumplimiento, Tecnológico, Imagen		1		1
Estratégico, Operativo, Cumplimiento		7		7
Estratégico, Operativo, Cumplimiento, Tecnológico, Imagen		3		3
Estratégico, Operativo, Tecnológico		2		2
Estratégico, Operativo, Tecnológico, Imagen		6		6
Estratégico, Tecnológico		3		3
Operativo	5	9		14
Operativo, Cumplimiento	2	8		10
Operativo, Cumplimiento, Tecnológico	1	3		4
Operativo, Cumplimiento, Tecnológico, Imagen	1	5		6
Operativo, Tecnológico	6	27	1	34
Operativo, Tecnológico, Imagen		7		7
Tecnológico	4	8		12
TOTAL GENERAL	**22**	**118**	**3**	**143**

Fuente de Información: archivo en formato Microsoft Excel Tabla Gestión Riesgos SDM Sep 2022

En la actualidad se encuentran monitoreando los activos de información que se tienen a cargo de la OTI, y para lo cual se en el cuadro anterior se resumen por agrupación de tipo de riesgo y se detalla el nivel de riesgo identificado, para lo cual aplican los controles que se tienen definidos en la NTC ISO 27001 del Anexo A, y su monitoreo se apoya con la gestión realizada del Operador.

FORTALEZAS.

Dentro del desarrollo de esta auditoría se observó:

- ✓ Disposición y colaboración brindada al equipo auditor por los profesionales, en la aplicación de las listas de verificación llevadas a cabo durante el desarrollo de la auditoría.
- ✓ Entrega oportuna de las evidencias y soportes solicitados en las fases de planeación y ejecución de la auditoría y la organización de esta; lo cual facilitó la gestión de evaluación por parte del equipo auditor.
- ✓ Compromiso y apoyo brindado por los profesionales designados como enlaces en el ejercicio de la auditoría.
- ✓ Se resalta el trabajo que ha venido desarrollando el Oficial de Seguridad, que, aunque no tiene un equipo de trabajo para desarrollar todo el tema se esfuerza por atender y dar cumplimiento a este tema.
- ✓ Las reuniones que realizan de manera semanal para hacer revisión de los diferentes temas, y con el fin de tomar acciones preventivas o correctivas de los temas tratados.
- ✓ Se participa en la 1ra Mesa de Infraestructura Critica del Distrito donde se realiza una jornada colaborativa orientada a la identificación de infraestructuras críticas de las entidades de publicas distritales.
- ✓ Se está pendiente de las directrices impartidas por MINTIC y Dirección de Gobierno Digital.

CONCLUSIONES.

Se concluye al revisar la aplicación de la Política de Seguridad de la Información, al interior de la entidad, se observa que esta se está cumplimiento de manera parcial, por lo que es

importante que todos los actores que hacen parte de esta política velen por la debida implementación y mantenimiento con el fin de salvaguardar la información que es el pilar de la operación de la entidad y que debe cumplir los atributos de confidencialidad, integridad y disponibilidad de la información.

RECOMENDACIONES

- Evaluar el nivel de obsolescencia de los equipos de cómputo con los que cuenta la entidad, con el fin de mejorar el rendimiento y garantizar que las herramientas tecnológicas para el desarrollo de las labores de la entidad.

- Efectuar sensibilizaciones sobre: "Consumir alimentos y bebidas, cerca de la plataforma tecnológica", con el fin de que todos los funcionarios tomen conciencia de los efectos y peligros de esta actividad; "Dejar los computadores encendidos en horas no laborables".

- Actualizar y formalizar los documentos que se aportaron en esta auditoría como borradores para mejorar la aplicación de la Política de Seguridad.

- Evaluar en llevar al sistema de calidad todos aquellos documentos se el operador ha venido trabajando y que impactan los servicios ofrecidos por la Oficina de Tecnologías de la Información y la Comunicación (Ejemplo: Procedimiento de Backups, entre otros).

- Realizar sensibilizaciones por parte de la OTI de manera continua para que todos los funcionarios y contratistas apropien la Política de Seguridad de la información y la aplicación de los controles para el prevenir los riesgos y asegurar los atributos de la información (integridad, disponibilidad y confiabilidad).

No obstante, es importante tener en cuenta la Ley 87 de 1993 "***Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones***" en sus artículos […]:

- Artículo 3**. Características del Control Interno**. Son características del Control Interno las siguientes: **a**. "*El Sistema de Control Interno forma parte integrante de los sistemas contables, financieros, de planeación, de información y operacionales de la respectiva entidad*; y, **c**. En cada área de la organización, el funcionario encargado

de dirigirla es responsable por control interno ante su jefe inmediato de acuerdo con los niveles de autoridad establecidos en cada entidad.

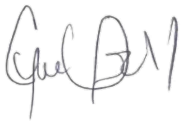
- Artículo 12. **Funciones de los auditores internos,** en su literal k) "*Verificar que se implanten las medidas respectivas recomendadas*" […].

Es importante mencionar, que la Oficina de Tecnologías de la Información y las Comunicaciones, es la responsable de formular y suscribir el Plan de Mejoramiento dentro de los diez (10) días hábiles siguientes a la comunicación de este Informe de acuerdo con el "*Instructivo Formulación y Seguimiento de Planes de Mejoramiento PV01- IN02, Versión: 1.0*" y remitirlo a la OCI.

Finalmente, se hace la salvedad que las posibles causas identificadas por los auditores de la OCI fueron las evidenciadas en el proceso auditor (no es una causa que se deba incluir de manera obligatoria en el plan de mejoramiento a suscribir), no obstante, los responsables de la ejecución de la operación de cada actividad, proyecto, programa o proceso auditado, deberán identificar la causa raíz de los hallazgos y observaciones configurados en esta auditoría, las cuales pueden ser diferentes a las inicialmente identificadas.

ANEXOS:
N/A

Nota[4]

Nombre(s) y firma(s) auditor(es):	Nombre y Firma del Responsable de la Auditoría (Jefe OCI)
 ANA YANCY URBANO VELASCO Profesional Especializado responsable de la verificación	 ALBA ENIDIA VILLAMIL MUÑOZ

[4] **Los informes en desarrollo de las auditorías deben ser:**

a) **Precisos** (Diga lo que tiene que decir. Es conveniente ser exacto (puntual) en cada frase y en el informe completo. Su redacción debe ser sencilla, clara, ordenada, coherente y en orden de importancia).
b) **Concisos** (La redacción debe ser breve, pero sin omitir lo relevante, la brevedad permite mayor impacto. Se debe buscar la forma de redactar los hallazgos en forma concreta, pero sin dejar de decir lo que se tiene que decir sobre la condición (situación detectada); asimismo, se debe incluir la fuente de criterio, el criterio de auditoría).
c) **Objetivo** (Todas las No Conformidades deben reflejar una situación real, manejada con criterios técnicos, analíticos e imparciales).
d) **Soportado** (Las afirmaciones, conceptos, opiniones y hallazgos, deben estar respaldadas con evidencia válida, suficiente, pertinente y competente).
e) **Oportuno** (Debe cumplir los términos de elaboración, consolidación, entrega, comunicación y publicidad).